IEEE 802.1AE-2006
&
IEEE 802.1X-2010
MACsec
Conformance Test Suite

Version 1.1

Technical Document

University of New Hampshire
InterOperability Laboratory
Bridge Functions Consortium

121 Technology Drive, Suite 2
Durham, NH 03824
Phone: (603) 862-3532
Fax: (603) 862-4181

http://www.iol.unh.edu/services/testing/bfc

MODIFICATION RECORD

- January 25th, 2008 – Initial Public Release
- August 8th 2010 – Revision to include 802.1X-2010 and a general overhaul of the tests

ACKNOWLEDGEMENTS

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite.

David Bond	University of New Hampshire
Nathan Bourgoine	University of New Hampshire
Aaron Stewart	University of New Hampshire
Timothy Carlin	University of New Hampshire

INTRODUCTION

Overview

The University of New Hampshire's InterOperability Laboratory (IOL) is an institution designed to improve the interoperability of standards based products by providing an environment where a product can be tested against other implementations of a standard. This suite of tests has been developed to help implementers evaluate the functionality of their IEEE 802.1AE-2006 and 802.1X-2010 based products. The tests do not definitively determine if a product conforms to the IEEE 802.1AE-2006 and 802.1X-2010 standards. Successful completion of all tests contained in this suite does not guarantee that the tested device will operate with other IEEE 802.1AE-2006 and 802.1X-2010 capable devices. However, combined with satisfactory operation in the UNH-IOL's interoperability test bed, these tests provide a reasonable level of confidence that the Device Under Test (DUT) will function well in many IEEE 802.1AE-2006 and 802.1X-2010 environments.

Organization of Tests

The tests contained in this document are organized to simplify the identification of information related to a test and to facilitate in the actual testing process. Each test contains an identification section that describes the test and provides cross-reference information. The discussion section covers background information and specifies why the test is to be performed. Tests are grouped in order to reduce setup time in the lab environment. Each test contains the following information:

Test Number

The Test Number associated with each test follows a simple grouping structure. Listed first is the Test Group Number followed by the test's number within the group. This allows for the addition of future tests to the appropriate groups of the test suite without requiring the renumbering of the subsequent tests.

Purpose

The purpose is a brief statement outlining what the test attempts to achieve. The test is written at the functional level.

References

The references section lists cross-references to the IEEE Std. 802.1AE-2006 and 802.1X-2010 standards and other documentation that might be helpful in understanding and evaluating the test and results.

Discussion

The discussion covers the assumptions made in the design or implementation of the test as well as known limitations. Other items specific to the test are covered here.

Test Setup

The setup section describes the configuration of the test environment. Small changes in the configuration should be included in the test procedure. The description and diagram included in the setup section is in the case that the DUT is a switch. If the DUT is an end station, the DUT will be connected directly to the testing station; for any test where this setup is modified for end stations, it will be specifically addressed in the setup section.

Procedure
The procedure section of the test description contains the step-by-step instructions for carrying out the test. It provides a cookbook approach to testing, and may be interspersed with observable results.

Observable Results
The observable results section lists specific items that can be examined by the tester to verify that the DUT is operating properly. When multiple values are possible for an observable result, this section provides a short discussion on how to interpret them. The determination of a pass or fail for a certain test is often based on the successful (or unsuccessful) detection of a certain observable result.

Possible Problems
This section contains a description of known issues with the test procedure, which may affect test results in certain situations.

TABLE OF CONTENTS

MODIFICATION RECORD 2

ACKNOWLEDGEMENTS 3

INTRODUCTION 4

TABLE OF CONTENTS 6

DEFAULT TEST SETUP 1

GROUP 1: PARAMETRIC TESTING 2

- TEST #1.1.1: TRANSMIT KEY CHANGE EVENT 3
- TEST #1.1.2: RECEIVE KEY CHANGE EVENT 4
- TEST #1.1.3: MACSEC PORT IMPLEMENTED 5
- TEST #1.1.4: POINT-TO-POINT PARAMETER SUPPORT 7
- TEST #1.2.1: TRANSMIT SECURE ASSOCIATION ASSIGNMENT 8
- TEST #1.2.2: TRANSMIT PACKET NUMBER VERIFICATION 9
- TEST #1.2.3: TRANSMIT SECURE CONNECTION IDENTIFIER ENCODING 10
- TEST #1.2.4: TRANSMIT ETHERTYPE ENCODING VERIFICATION 12
- TEST #1.2.5: ENCRYPTION BIT VERIFICATION 13
- TEST #1.2.6: CHANGED TEXT BIT VERIFICATION 14
- TEST #1.2.7: TRANSMIT ASSOCIATION NUMBER ENCODING 15
- TEST #1.2.8: TRANSMIT SHORT LENGTH FIELD VERIFICATION 16
- TEST #1.2.9: TRANSMIT ES BIT VERIFICATION 18
- TEST #1.2.10: SECURITY TAG VERSION NUMBER 19
- TEST #1.3.1: RECEIVE ETHERTYPE IDENTIFICATION 20
- TEST #1.3.2: RECEIVED VERSION NUMBER BEHAVIOR 22
- TEST #1.3.3: RECEIVED ES BIT VERIFICATION 24
- TEST #1.3.4: RECEIVED SC BIT VERIFICATION 26
- TEST #1.3.5: RECEIVE ASSOCIATION NUMBER VERIFICATION 28
- TEST #1.3.6: RECEIVED SHORT LENGTH VERIFICATION 29
- TEST #1.3.7: RECEIVE PACKET NUMBER VERIFICATION 30

DEFAULT TEST SETUP

Unless specified otherwise, all MACsec connections will be configured with the following settings.

Default Bridge Settings for DUT

Parameter	**Value**
Bridge VLANs	Default VLAN only (VID 1)
Spanning Tree operational state	Disabled
GMRP operational state	Disabled
GVRP operational state	Disabled
IP routing	Disabled
Filtering Database Aging Time	300 seconds

Default Port Settings for DUT

Parameter	**Value**
Acceptable Frame Types	Admit All Frames
Duplex	Full Duplex
Enable Ingress Filtering	Reset
Port VLAN membership	Default VLAN only
PVID	1

Default MACsec Settings for DUT

Parameter	**Value**
adminPointToPointMAC	Auto
Encryption	Enabled
alwaysIncludeSCI	False
useSCB	False
protectFrames	True
Cipher Suit	Default

Default Keys

Key	**Value**
Pre-shared CAK (if MKA is supported)	0x42524944474520465 54E4354494F4E53
	"BRIDGE FUNCTIONS" (ASCII)
SAK (if MKA is not supported)	0x42524944474520465 54E4354494F4E53
	"BRIDGE FUNCTIONS" (ASCII)

GROUP 1: PARAMETRIC TESTING

Scope: The following tests cover parametric tests specific to the electrical interface of an IEEE 802.1AE-2006 and 802.1X-2010 device.

Overview: The following group of tests pertains to the determination of various parametric values as defined in IEEE Std. 802.1AE-2006 and 802.1X-2010. Note, successfully passing these tests, or failing these tests does not necessarily indicate that the DUT will, or will not, be interoperable. Devices that pass these tests are more inclined to be interoperable with, not only existing products, but also all future standard compliant devices.

Test #1.1.1: Transmit Key Change Event

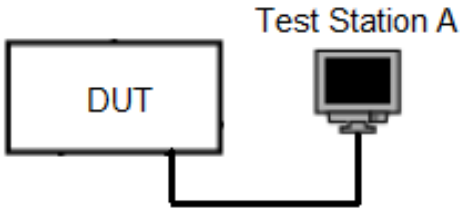
Purpose: To verify that DUT is capable of receiving and installing a new key in an appropriate amount of time.

Reference:

- IEEE Std. 802.1AE-2006 Clause 8.2.2

Discussion: During communications between devices involved in a secured channel, the keys used by the devices will occasionally be changed. This process of changing keys should not cause problems in the link, and should occur in a timely fashion. Correct operation is important for both transmitters and receivers. When transmitting a new key, the transmitting device should be able to handle a maximum length delay by the secure channel partner implementing the new key.

Test Setup: Connect the DUT to the testing station.



Procedure:

1. Establish a secure connection with the DUT.
2. Transmit ICMP echo requests to the DUT continuously with incrementing data in the data field.
3. Upon reception of a new key, wait for one second and then begin using the new key.
4. Observe the value of the data in the ICMP echo response frames.

Observable Results:

a. The DUT should not drop any of the ICMP echo request frames due to the key change event.

Possible Problem: None

Test #1.1.2: Receive Key Change Event

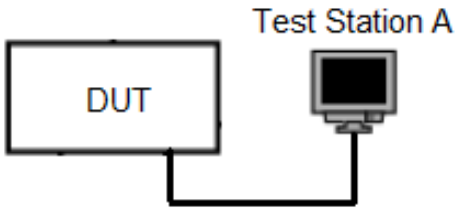
Purpose: To verify that DUT is capable of receiving and installing a new key in an appropriate amount of time.

Reference:

- IEEE Std. 802.1AE-2006 Clause 8.2.2

Discussion: During communications between devices involved in a secured channel, the keys used by the devices will occasionally be changed. This process of changing keys should not cause problems in the link, and should occur in a timely fashion. Correct operation is important for both transmitters and receivers. When receiving a new key, the receiving device should take less than the maximum length delay to implementing the new key.

Test Setup: Connect the DUT to the testing station.



Procedure:

1. Establish a MACsec connection with the DUT.
2. Transmit ICMP echo requests to the DUT continuously with incrementing data in the data field.
3. Transmit a new key to the DUT.
4. Observe the value of the data in the ICMP echo response frames.

Observable Results:

a. The DUT should begin using the new key within one second plus the transmit time for a minimum size frame.

Possible Problem: The standard specifies that the time taken shall be from when the Cipher Suite receives the key from the Key Agreement Entity. This time is not equal to the time when the new key was transmitted to the DUT.

Test #1.1.3: MACsec Port Implemented

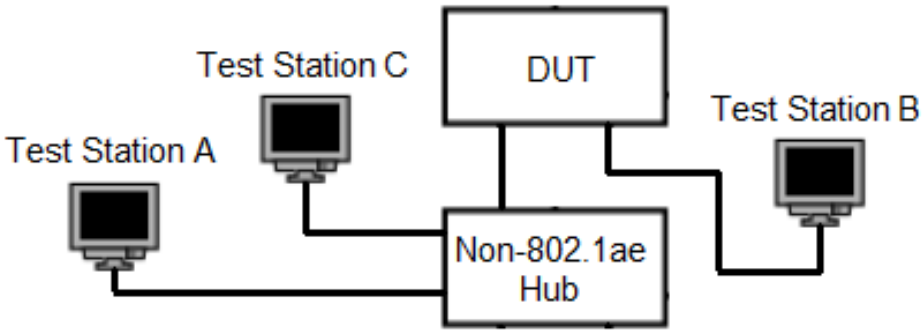
Purpose: To verify that the DUT implements the controlled and uncontrolled ports used for transmission and reception of MACsec frames.

References:

- IEEE Std 802.1AE – 2006 Clauses 5.3

Discussion: Devices implementing 802.1AE MACsec implement both a controlled and an uncontrolled port within the device. These ports both communicated via the common port to the outside world, and are used depending on the circumstances of the traffic to be transmitted. Traffic should be observable from both the controlled and uncontrolled port in the form of frames that contain security information and those that do not. Incorrect implementation of these ports could cause issues for devices while setting up security associations and maintaining a secured link.

Test Setup: For switches and end stations, connect the DUT, testing station A, and testing station C to the shared medium hub. If the DUT is a switch, also connect testing station B to the DUT.



Procedure:

If the DUT is a switch:

1. Establish secure associations between testing station A, B, and the DUT.
2. Transmit frames from testing station B with a destination of testing station A.
3. Observe the frames received by testing station A.
4. Transmit frames from testing station B with a destination of testing station C.
5. Observe the frames received by testing station C.

If the DUT is an end station:

6. Establish secure associations between testing station A, and the DUT.
7. Transmit ICMP Echo Requests to the DUT from testing station A.
8. Observe the response received by testing station A.
9. Transmit ICMP Echo Requests to the DUT from testing station C.
10. Observe the response received by testing station C.

Observable Results:

a. In steps 3 and 8, the DUT should transmit secured frames.
b. In steps 5 and 10, the DUT should transmit unsecured frames.

Possible Problems: None

Test #1.1.4: Point-to-Point parameter support

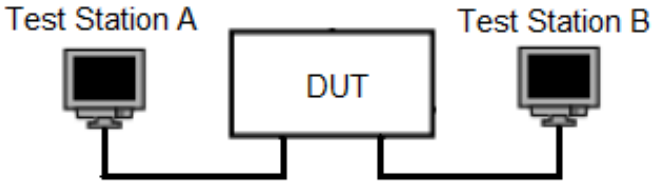
Purpose: To verify that the DUT supports operating a port in point-to-point mode.

References:

- IEEE Std 802.1AE – 2006 Clauses 5.3, 6.5, and 9.5

Discussion: In some situations, a device may determine that a link is a point-to-point connection with another host. This allows for special considerations to be taken on that port when doing various operations. In the case of MACsec, knowing that the link is point-to-point allows the protocol to avoid using an explicitly encoded SCI. When transmitting frames to a port that is set as a point-to-point link, the MACsec entity should associate the frame with the implicit SCI for the connection.

Test Setup: Connect DUT to the testing stations.



Procedure:

1. Establish secure associations between the testing stations A, B, and the DUT.
2. Transmit frames from testing station A to testing station B using ES=0, SC=0, and with no SCI.
3. Observe the frames received at testing station B.
4. Observe the point-to-point state of the port in management.

Observable Results:

a. In step 3, testing station B should receive all frames transmitted by testing station A.
b. In step 4, the management should correctly reflect the point-to-point status of the connection.

Possible Problems: The DUT may not give the ability to check the management for point-to-point status. This Test cannot be run if the DUT is an end station.

Test #1.2.1: Transmit Secure Association Assignment

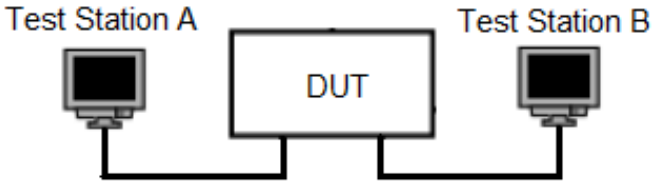
Purpose: To verify that the DUT correctly assigns the Secure Association number to frames during the Secure Frame Generation process.

Reference:

- IEEE Std 802.1AE – 2006 Clause 10.5

Discussion: During the transmit process, frames that are to be protected must be assigned the correct Secure Association (SA) and encoded with the correct Association Number (AN). This value will change periodically during the existence of a Secure Channel (SC) and must be reflected in the SecTAG header information. Failure to do this operation will result in communications failures between devices.

Test Setup: Connect the DUT to the testing stations.



Procedure:

If the DUT is a switch:

1. Establish secure associations between testing station A, B, and the DUT.
2. Transmit frames from testing station B to testing station A.
3. Observe the frames received by testing station A.
4. Transmit a new egress key to the DUT for testing station A.
5. Transmit frames from testing station B to testing station A.
6. Observe the frames received by testing station A.

If the DUT is an end station:

7. Establish secure associations between testing station A and the DUT.
8. Transmit ICMP Echo Requests from testing station A to the DUT.
9. Observe the frames received by testing station A.
10. Transmit a new egress key to the DUT.
11. Transmit frames from testing station A to the DUT.
12. Observe the frames received by testing station A.

Observable Results:

a. In step 3, 6, 9, and 12, the testing stations should receive the frames transmitted by the DUT with the correct Association Number.

Possible Problems: None

Test #1.2.2: Transmit Packet Number Verification

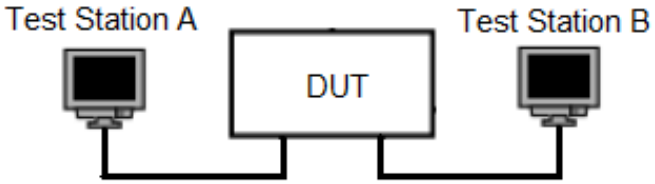
Purpose: To verify that the DUT properly assigns the packet number for each frame transmitted during a secure association.

Reference:

- IEEE Std 802.1AE – 2006 Clause 10.5

Discussion: To protect against frames being repeated on the network, each frame is assigned a packet number (PN). The packet number should be encoded with a number unique for the secure association (SA) currently in use. The packet number should increment once per frame transmitted on the controlled port. If the SA exists long enough for the packet counter to reach 2^{32}-1, the controlled port should become non-operational.

Test Setup: Connect the DUT to testing stations.



Procedure:

If the DUT is a switch:

1. Establish secure associations between testing station A, B, and the DUT.
2. Transmit enough frames from testing station B to testing station A to overflow the 32 bit PN counter.
3. Observe the frames received by testing station A.
4. Transmit a secured frame from testing station A to testing station B.
5. Observe the frames received by testing station B.

If the DUT is an end station:

6. Establish secure associations between testing station A and the DUT.
7. Transmit enough ICMP Echo Requests from testing station A to the DUT to overflow the 32 bit PN counter.
8. Observe the frames received by testing station A.

Observable Results:

a. In steps 3 and 8, the DUT should stop transmitting secured frames once the PN has reached its maximum value. The last secured frame observed to be transmitted by the DUT should have a packet number of 4,294,967,295 (0xFFFFFFFF).
b. In step 5, testing station B should not receive the frames.

Possible Problems: None

Test #1.2.3: Transmit Secure Connection Identifier Encoding

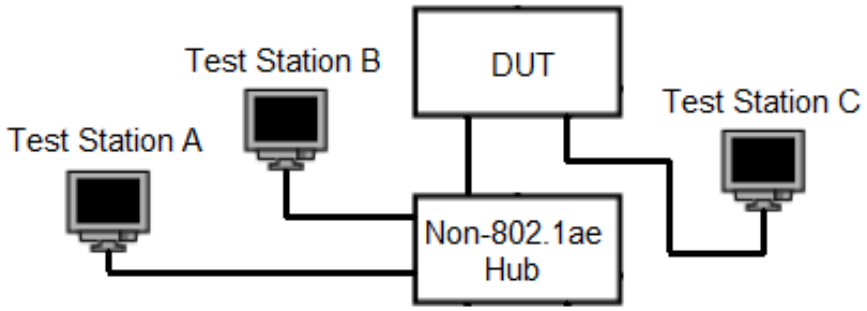
Purpose: To verify that the DUT properly assigns a unique Secure Connection Identifier (SCI) to secure connections within a secure Community Association (CA)

Reference:

- IEEE Std 802.1AE – 2006 Clause 10.5

Discussion: Secure connections between devices can be defined by either an implicit, or explicitly by using a secure connection identifier (SCI). In the case of point-to-point and links with an end station, the SCI may be implied by the flow of traffic. In other cases, the SCI within a frame will contain the unique identifier for that secure connection. This is apparent when there are multiple devices within a CA, each with a unique secure connection (SC) to another device in the CA.

Test Setup: For switches and end stations, connect the DUT, testing station A, and testing station B to the shared medium hub. If the DUT is a switch, also connect testing station C to the DUT.



Procedure:

If the DUT is a switch:

1. Establish secure associations between testing station A, B, C, and the DUT.
2. Transmit frames from testing station C to testing stations A and B.
3. Observe the frames received by testing station A.
4. Observe the frames received by testing station B.
5. Transmit frames from testing station A to testing station C.
6. Transmit frames from testing station B to testing station C.
7. Observe the frames received by testing station C.

If the DUT is an end station:

8. Establish secure associations between testing station A, B, and the DUT.
9. Transmit ICMP Echo Requests from testing station A to the DUT.
10. Observe the frames received by testing station A.
11. Transmit ICMP Echo Requests from testing station B to the DUT.
12. Observe the frames received by testing station B.

Observable Results:

a. In all observed cases, the frames received by the testing stations should contain the correct SCI for the secure connection the frame was transmitted over.

Possible Problems: None

Test #1.2.4: Transmit EtherType Encoding Verification

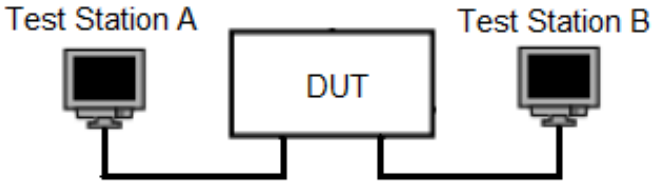
Purpose: To verify that the DUT properly encodes the Ethernet length/type field of the Security Tag during the transmit operation.

Reference

- IEEE Std 802.1AE – 2006 Clause 9.4

Discussion: Frames that are protected using the MACsec system must be identified as such in order for them to be treated appropriately by network devices. In order to uniquely identify this type of frames, an Ethernet type/length field value has been assigned for IEEE 802.1ae. Failing to encode a frame with this type/length value will cause the frame to not be recognized as a security enhanced frame.

Test Setup: Connect the DUT to the testing stations.



Procedure:

If the DUT is a switch:

1. Transmit secured frames from testing station A to testing station B.
2. Observe the frames received by testing station B.

If the DUT is an end station:

3. Transmit secured ICMP Echo Requests to the DUT from testing station A.
4. Observe the frames received by testing station A.

Observable Results:

a. In steps 2 and 4, the length/type field in all secured frames should be 88-E5 (hex).
b. In steps 2 and 4, the unsecured type length/type field should appear after the end of the security tag.

Possible Problems: None

Test #1.2.5: Encryption Bit Verification

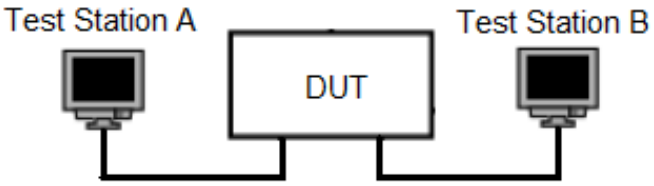
Purpose: To verify that the TCI field Encryption bit in the security tag is correctly encoded.

Reference

- IEEE Std 802.1AE – 2006 Clause 9.5

Discussion: Secured frames may be protected in two ways. Frames could have integrity protection only, in which the data remains unencrypted. Frames could also be encrypted to protect the contents of the packet from observation by a third party. If encryption is used, this must be indicated by the receiver though the use of the E bit in the TCI section of the SecTAG header.

Test Setup: Connect the DUT to the testing stations.



Procedure:

If the DUT is a switch:

1. Configure the DUT to use encryption on the port attached to testing station A.
2. Transmit frames from testing station B to testing station A.
3. Observe the frames received by testing station A.
4. Configure the DUT to not use encryption on the port attached to testing station A.
5. Transmit frames from testing station B to testing station A.
6. Observe the frames received by testing station A.

If the DUT is an end station:

7. Configure the DUT to use encryption on the port attached to testing station A.
8. Transmit ICMP Echo Requests to the DUT from testing station A.
9. Observe the frames received by testing station A.
10. Configure the DUT to not use encryption on the port attached to testing station A.
11. Transmit ICMP Echo Requests to the DUT from testing station A.
12. Observe the frames received by testing station A.

Observable Results:

a. In steps 3 and 9, the E bit of the TCI should equal 1.
b. In steps 6 and 12, the E bit of the TCI should equal 0.

Possible Problems: None

Test #1.2.6: Changed Text Bit Verification

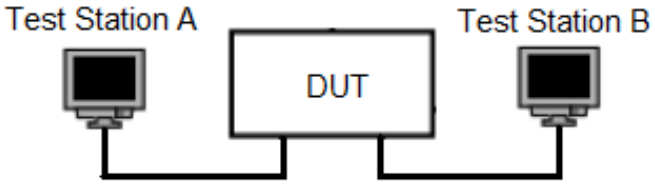
Purpose: To verify that the TCI field Changed Text bit is correctly set for secured frames.

Reference

- IEEE Std 802.1AE – 2006 Clause 9.5
- IEEE Std 802.1AE – 2006 Clause 14

Discussion: Frames being secured can be protected though integrity verification and as encryption. Both do not need to be used. In order to indicate that the text of an unencrypted frame has been changed from the original UserData the C bit should be set. This should occur if an ICV that is not 16 bytes is used or if the frame's data field has been modified. Failing to properly encode this bit could cause a host to incorrectly decide that a frame had been corrupted.

Test Setup: Connect the DUT to the testing stations.



Procedure:

If the DUT is a switch:

1. Configure the DUT to use only integrity protection on the port attached to testing station A.
2. Transmit frames from testing station B to testing station A.
3. Observe the frames received by testing station A.
4. Configure the DUT to use encryption on the port attaching testing station A.
5. Transmit frames from testing station B to testing station A.
6. Observe the frames received by testing station A.

If the DUT is an end station:

7. Configure the DUT to use only integrity protection on the port attaching testing station A.
8. Transmit ICMP Echo Requests to the DUT from testing station A.
9. Observe the frames received by testing station A.
10. Configure the DUT to not use encryption on the port attaching testing station A.
11. Transmit ICMP Echo Requests to the DUT from testing station A.
12. Observe the frames received by testing station A.

Observable Results:

a. In step 3, the forwarded frames should have the C bit set to 0.
b. In step 6, the forwarded frames should have the C bit set to 1.
c. In step 9, the ICMP Echo Responses should have the C bit set to 0.
d. In step 12, the ICMP Echo Responses should have the C bit set to 1.

Possible Problems: None

Test #1.2.7: Transmit Association Number Encoding

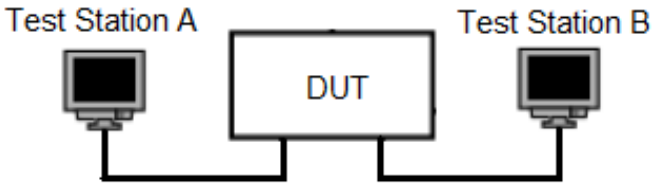
Purpose: To verify that the DUT correctly encodes a new Association Number (AN) when switching to a new Secure Association (SA).

Reference

- IEEE Std 802.1AE – 2006 Clause 7.1.3

Discussion: Devices communicating over a secure link will go though a series of secure associations (SA) within a single secure connection (SC). This will occur when a new key is exchanged by the Key Agreement Entities (KaY) on the devices. After exchange of such a key, a new SA is created and the SC is moved to this new SA. To indicate the switch from the old to the new SA, the association number (AN) encoded in the frames is changed to the AN for the new SA. Failure to correctly encode the AN on transmit will cause the receiving station to attempt validation/decryption with an incorrect key. This will result in the frames being marked as corrupted, and a loss of data will be observed.

Test Setup: Connect the DUT to the testing stations.



Procedure:

If the DUT is a switch:

1. Transmit frames from testing station B to testing station A.
2. Observe the AN field of the frames received by testing station A.
3. Establish a new SA with testing station A on the DUT.
4. Observe the AN field of the frames received by testing station A.
5. Repeat steps 3 and 4 three times.

If the DUT is an end station:

6. Source ICMP Echo Requests from testing station A to the DUT.
7. Observe the AN field of the ICMP Echo Replies received by testing station A.
8. Establish a new SA with testing station A on the DUT.
9. Observe the AN field of the ICMP Echo Replies received by testing station A.
10. Repeat steps 8 and 9 three times.

Observable Results:

a. In steps 4 and 9, the DUT should change the AN encoded in the frames to the AN associated with the new SA.

Possible Problems: None

Test #1.2.8: Transmit Short Length Field Verification

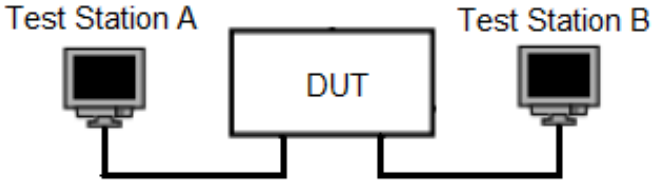
Purpose: To verify that a DUT correctly sets the Short Length field in the SecTAG.

Reference:

- IEEE Std. 802.1AE-2006 Clause 9.7

Discussion: Devices implementing MACsec may have to send frames that have a small data payload associated with them. In this case, the frame may be padded out to cope with minimum frame size restrictions on the network. The Short Length field specifies the number of bytes between the end of the data and the beginning of the ICV field. This acts the same way a Length field in a conventional Ethernet frame works. Incorrect encoding of these fields will cause the frame to be interpreted wrong, and mostly likely be judged as invalid by the recipient. This would cause serious interoperability issues for devices exhibiting this behavior.

Test Setup: Connect the DUT to the testing stations.



Procedure:

If the DUT is a switch:

1. Establish secure connections between the DUT and the testing stations.
2. Transmit frames with a payload of 1 byte from testing station A with a destination of testing station B.
3. Observe the Short Length field in the SecTAG of the frame received by testing station B.
4. Repeat steps 3 and 4 for payload lengths of 2 though 48 Bytes.

If the DUT is an end station:

5. Establish a secure connection between testing station A and the DUT.
6. Transmit ICMP Echo requests to the DUT with payload sizes of 1 byte.
7. Observe the Short Length field of the frames received by testing station A.
8. Repeat steps 6 and 7 for payload lengths of 2 through 20 bytes.

Observable Results:

a. In step 3, the DUT should forward all frames with the correct Short Length field encoding.
b. In step 7, the DUT should respond to all frames with the correct Short Length field encoding.
c. In all cases, bits 7 and 8 of the Short Length field should be zero.

Possible Problems: When testing a DUT that is an end station and using ICMP Echo Requests, the minimum data size that can be sent is 28 bytes (only IP/ICMP headers). This leaves the possibility that a DUT could have an undetected issue with data payloads smaller than 28 bytes.

Test #1.2.9: Transmit ES Bit Verification

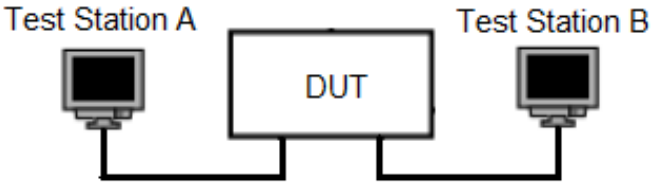
Purpose: To verify that DUT correctly sets the ES and SC bits if the device is an end station.

Reference:

- IEEE Std. 802.1AE-2006 Clause 9.5

Discussion: A device may set the end station (ES) bit when using an SCI in which the first 6 octets are equal to the devices source MAC address. If this is the case, the device should not set the SC bit and does not explicitly encode the SCI in the SecTAG. If the SC bit is set in the TCI, the DUT should not set the ES bit.

Test Setup: Connect the DUT to a secure channel partner



Procedure:

If the DUT is a switch:

1. Establish a secure connection to the DUT from the testing stations.
2. Transmit frames from testing station A to testing station B.
3. Observe the ES and SC bits in the SecTAG of the frame received by testing station B.

If the DUT is an end station:

4. Establish a secure connection between testing station A and the DUT.
5. Transmit Echo requests from testing station A to the DUT.
6. Observe the ES and SC bits in the SecTAG of the frames received by testing station A.

Observable Results:

a. In step 3, the DUT should not set the ES bit of the SecTAG.
b. In step 6, if the DUT sets the ES bit, the SC bit should be clear.

Possible Problem: None

Test #1.2.10: Security Tag Version Number

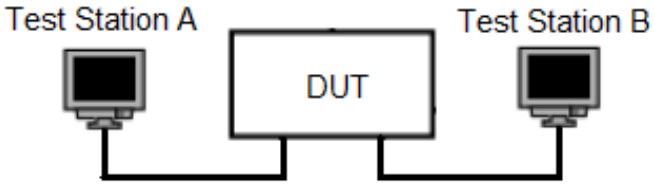
Purpose: To verify that DUT uses an appropriate version number encoded in the SecTAG.

Reference:

- IEEE Std. 802.1AE-2006 Clause 9.5

Discussion: Devices implementing 802.1AE MACsec should use an appropriate value in the SecTAG to convey which version of MACsec they are using. Incorrect version numbers may cause devices to not interoperate due to mismatched versions. Currently only one value is acceptable for the MACsec version.

Test Setup: Connect the DUT to a secure channel partner.



Procedure:

If the DUT is a switch:

1. Establish a secure connection to the DUT from the testing stations.
2. Transmit frames from testing station A to testing station B.
3. Observe the version bit in the SecTAG of the frames received by testing station B.

If the DUT is an end station:

4. Establish a secure connection between testing station A and the DUT.
5. Transmit Echo requests from testing station A to the DUT.
6. Observe the version bit in the SecTAG of the frames received by testing station A.

Observable Results:

a. In all received frames, the version number observed should be 0.

Possible Problem: None

Test #1.3.1: Receive EtherType Identification

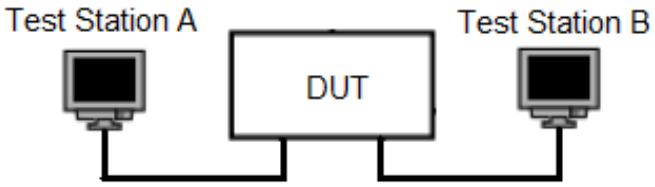
Purpose: To verify that the DUT correctly recognizes frames encoded with and without a SecTAG and passes the frames to the controlled port and uncontrolled ports respectively.

Reference

- IEEE Std 802.1AE – 2006 Clauses 9.3 and 10.6

Discussion: After a frame has been received and its FCS verified, the frame must be processed according to what type of frame it is. The EtherType field is often used to determine what type of frame was received. This instructs the receiving device to treat it as an IP, ARP, VLAN, or many other types of frame. For MACsec the defined EtherType is 88-E5 in hexadecimal. Frames received with this EtherType should be processed and, assuming the frame was valid, sent to the Controlled port. Frames without this EtherType should be sent directly to the Uncontrolled port. Incorrect steering of frames by the input duplexer may cause issues when interoperating with other devices.

Test Setup: Connect the DUT to the testing stations.



Procedure:

If the DUT is a switch:

1. Transmit correctly formed MACsec frames from testing station A to testing station B.
2. Observe the frames received by testing station B.
3. Transmit frames with an EtherType of 88-E5 from testing station A to testing station B that are not MACsec encoded frames.
4. Observe the frames received by testing station B.
5. Transmit MACsec encoded frames with an EtherType of 88-E4.
6. Observe the frames received by testing station B.
7. Repeat steps 5 and 6 for an EtherType of 88-E6.

If the DUT is an end station:

8. Transmit correctly formed MACsec ICMP Echo Requests from testing station A to the DUT.
9. Observe the responses from the DUT.
10. Transmit ICMP Echo Requests with an EtherType of 88-E5 from testing station A to the DUT that are not MACsec encoded frames.
11. Observe the frames received by testing station A.
12. Transmit MACsec encoded ICMP Echo Requests with an EtherType of 08-00 from testing station A to the DUT.
13. Observe the frames received by testing station A.

14. Repeat steps 12 and 13 for an EtherType of 88-E6.

Observable Results:

a. In step 2, the DUT should forward the transmitted frames to testing station B.
b. In step 4, the DUT should not forward the frames.
c. In steps 6 and 7, the DUT should forward the frames to testing station B without stripping off the MACsec information contained within the frames.
d. In step 9, the DUT should respond to the ICMP Echo Requests with an ICMP Echo Response.
e. In step 11, the DUT should not respond to the ICMP Echo Requests.
f. In step 13, the DUT should not respond to the ICMP Echo Requests.

Possible Problems: None

Test #1.3.2: Received Version Number Behavior

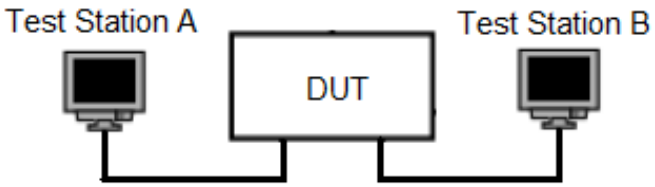
Purpose: To observe the behavior of the DUT when receiving a version number that is not the allowed version.

Reference

- IEEE Std 802.1AE – 2006 Clause 9.5

Discussion: In the current specification for MAC security, the only allowable version number for a properly encoded frame is zero (0). This test is intended to observe the behavior of a device when a version number of one (1) is received. Though this should not occur, this may become relevant with future versions of the specification, or with devices that are not behaving correctly. The standard is non-specific about what the correct behavior is when receiving the wrong version number.

Test Setup: Connect the DUT to testing station A. If the DUT is a switch, connect testing station B to a separate port on the DUT.



Procedure:

If the DUT is a switch:

1. Transmit MACsec frames with the version number bit clear from testing station A to testing station B.
2. Observe the frames received by testing station B.
3. Transmit MACsec frames with the version number bit set from testing station A to testing station B.
4. Observe the frames received by testing station B.

If the DUT is an end station:

5. Transmit MACsec protected ICMP Echo Requests with the version bit clear from testing station A to the DUT.
6. Observe the frames received by testing station A.
7. Transmit MACsec protected ICMP Echo Requests with the version bit set from testing station A to the DUT.
8. Observe the frames received by testing station A.

Observable Results:

a. In step 2, the DUT should forward the frame to testing station B.
b. In step 4, the DUT should not forward the frame to testing station B.
c. In step 6, the DUT should respond with an ICMP Echo Reply.
d. In step 8, the DUT should not respond with an ICMP Echo Reply.

Possible Problems: None

Test #1.3.3: Received ES Bit Verification

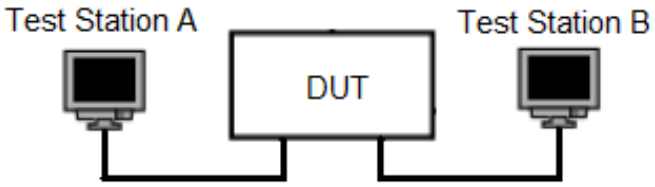
Purpose: To verify that the DUT correctly recognizes the End Station (ES) bit in an incoming frame.

Reference

- IEEE Std 802.1AE – 2006 Clause 9.5

Discussion: An end station device may use the end station bit to indicate to the link partner that the device is an end station and that the SCI is not explicitly encoded in the frame. If the ES bit is set, the SC bit must be clear for the frame to be valid. Like the point-to-point case, the SCI is omitted from the frame entirely. In this case, the receiving SecY should use an SCI equal to the frame's source MAC address. The receiving SecY should use a Port Identifier of 00-01. Failure to use the source MAC address System Identifier field could cause a device to associate a frame with the wrong Secure Channel.

Test Setup: Connect the DUT to testing station A. If the DUT is a switch, connect testing station B to a separate port on the DUT.



Procedure:

If the DUT is a switch:

1. Transmit frames from testing station A to testing station B with no SCI, a source MAC address that is equal to the first six bytes of the SCI for testing station A and with ES=1 and SC = 0.
2. Observe the frames received at testing station B.
3. Transmit frames from testing station A to testing station B with a source MAC address that is equal to the first six bytes of the SCI for testing station A and with ES=1 and SC = 1 and with an SCI included.
4. Observe the frames received at testing station B.

If the DUT is an end station:

5. Transmit ICMP Echo Requests from testing station A to the DUT with no SCI, a source MAC address that is equal to the first six bytes of the SCI for testing station A and with ES=1 and SC = 0.
6. Observe the frames received by testing station A.
7. Transmit ICMP Echo Requests from testing station A to the DUT with a source MAC address that is equal to the first six bytes of the SCI for testing station A and with ES=1 and SC = 1 and with an SCI included.
8. Observe the frames received by testing station A.

Observable Results:

a. In step 2, the DUT should forward the frame to testing station B.
b. In step 4, the DUT should not forward the frame to testing station B.
c. In step 6, the DUT should reply to the ICMP Echo Requests.
d. In step 8, the DUT should not reply to the ICMP Echo Requests.

Possible Problems: None

Test #1.3.4: Received SC Bit Verification

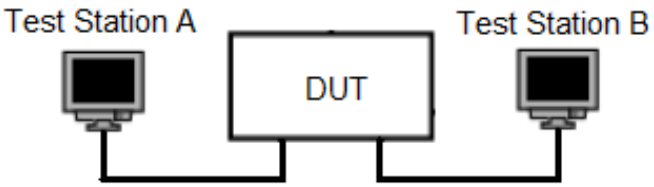
Purpose: To verify that the DUT observes the encoded SCI when the SC bit is set.

Reference

- IEEE Std 802.1AE – 2006 Clause 9.5, 10.5.3

Discussion: The Secure Connection (SC) bit is intended to convey that the SCI has been explicitly encoded in the SecTAG of the frame. This is not particularly important when the connection between devices is point-to-point, or if the device is an end station device. In those cases the SCI is not explicitly encoded in the frame. A device that is in one of those two configurations should still examine the SCI if the SC bit is set on received frames. Failure to do this could cause interoperability problems between devices.

Test Setup: Connect the DUT to testing station A. If the DUT is a switch, connect testing station B to a separate port on the DUT. Confirm that the connections between devices are point-to-point.



Procedure:

If the DUT is a switch:

1. Transmit frames from testing station A to testing station B with the SC bit clear and no SCI encoded in the frame.
2. Observe the frames received by testing station B.
3. Transmit frames from testing station A to testing station B with the SC bit set and the SCI correctly encoded in the SecTAG.
4. Observe the frames received by testing station B.
5. Transmit frames from testing station A to testing station B with the SC bit set and an incorrect SCI encoded in the SecTAG.

Observe the frames received by testing station B.

If the DUT is an end station:

6. Transmit ICMP Echo Requests from testing station A to the DUT with the SC bit clear and no SCI encoded in the frame.
7. Observe the frames received by testing station A.
8. Transmit ICMP Echo Requests from testing station A to the DUT with the SC bit set and the SCI correctly encoded in the SecTAG.
9. Observe the frames received by testing station A.
10. Transmit ICMP Echo Requests from testing station A to the DUT with the SC bit set and an incorrect SCI encoded in the SecTAG.
11. Observe the frames received by testing station A.

Observable Results:

a. In steps 2 and 4, the DUT should forward the transmitted frames to testing station B.
b. In step 6, the DUT should not forward the frames.
c. In steps 8 and 10, the DUT should respond to the ICMP Echo Requests.
d. In step 12, the DUT should not respond to the ICMP Echo Requests.

Possible Problems: None

Test #1.3.5: Receive Association Number Verification

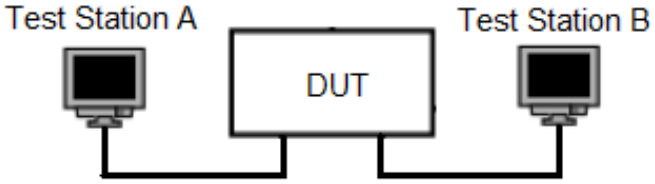
Purpose: To verify that the DUT correctly assigns received frames to the specified association number.

Reference

- IEEE Std 802.1AE – 2006 Clause 9.6

Discussion: Devices participating in a secure connection (SC) must change the secure association (SA) that is being used periodically. The SA that is being used to talk to a host is encoded in the header of the frame to allow the receiver to know which key to use when validating and decoding frames. If the device receiving the frame does not correctly assign the frame to the indicated SA, the frame will not be correctly decoded and will be lost.

Test Setup: Connect the DUT to testing station A. If the DUT is a switch, connect testing station B to a separate port on the DUT.



Procedure:

If the DUT is a switch:

1. Transmit frames from testing station A to testing station B with an appropriate AN encoded in the frame.
2. Observe the frames received at testing station B.
3. Transmit frames from testing station A to testing station B with an inappropriate AN.
4. Observe the frames received at testing station B.

If the DUT is an end station:

5. Transmit ICMP Echo Requests from testing station A to the DUT with an appropriate AN.
6. Observe the frames received by testing station A.
7. Transmit ICMP Echo Requests from testing station A to the DUT with an inappropriate AN.
8. Observe the frames received by testing station A.

Observable Results:

a. In step 2, the DUT should forward the frames to testing station B.
b. In step 4, the DUT should not forward the frames to testing station B.
c. In step 6, testing station A should receive an ICMP Echo Reply from the DUT.
d. In step 8, testing station A should not receive an ICMP Echo Reply from the DUT.

Possible Problems: None

Test #1.3.6: Received Short Length Verification

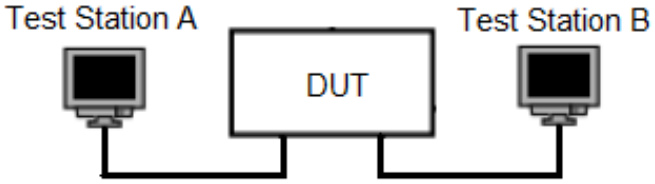
Purpose: To verify that the DUT correctly decodes and uses the short length field of the SecTAG header.

Reference

- IEEE Std 802.1AE – 2006 Clause 9.7

Discussion: During the course of a secure channel's existence, it is likely that UserData will be sent on this link that are smaller than the minimum payload size for the network link. When this occurs, the frame will require padding. In a MACsec frame, the length of the original data is indicated by the Short Length (SL) field. Failure to correctly decode and apply this value will result in portions of padding or data being incorrectly included/excluded from the UserData.

Test Setup: Connect the DUT to testing station A. If the DUT is a switch, connect testing station B to a separate port on the DUT.



Procedure:

If the DUT is a switch:

1. Transmit a frame from testing station A to testing station B with a payload size of 1 byte.
2. Observe the frames received by testing station B.
3. Repeat steps 1 and 2 for payloads of 2 though 48 bytes.

If the DUT is an end station:

4. Transmit an ICMP Echo Request frame with 1 byte of data to the DUT from testing station A.
5. Observe the response from the DUT.
6. Repeat steps 4 and 5 for ICMP Echo Request data sizes of 2 though 20 Bytes.

Observable Results:

a. In step 2, the DUT should forward the frames to testing station B. The payload size should be unchanged from the frames transmitted from testing station A.
b. In steps 4, the DUT should reply with ICMP Echo Replies having a short length corresponding to the original request.

Possible Problems: When testing a DUT that is an end station and using ICMP Echo Requests, the minimum data size that can be sent is 28 bytes (only IP/ICMP headers). This leaves the possibility that a DUT could have an undetected issue with data payloads smaller than 28 bytes.

Test #1.3.7: Receive Packet Number Verification

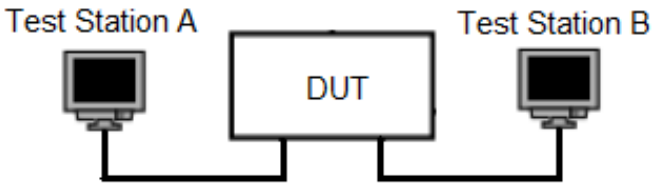
Purpose: To verify that the DUT properly verifies the packet number located in the received frame.

Reference

- IEEE Std 802.1AE – 2006 Clause 9.8, 10.6.2, 10.6.4

Discussion: An important feature of securing a network is ensuring that the frames are not being duplicated and spoofed by an attacker, and to ensure that a malfunctioning device does not cause harm to the network. One step taken to prevent this is to include a packet number (PN) that allows for tracking of layer 2 conversations on the network. This will quickly show if a frame is being duplicated and sent onto the network. MACsec devices expect to receive a certain sequence of PNs for a given secure association (SA), and use a replayWindow to allow some level of unordered delivery. Frames received outside of this window indicate a possible problem on the network.

Test Setup: Connect the DUT to testing station A. If he DUT is a switch, connect testing station B to a separate port on the DUT.



Procedure:

If the DUT is a switch:

1. Transmit a frame from testing station A to testing station B with a PN that is the correct next number for that SA.
2. Observe the frames received by testing station B.
3. Transmit a frame from testing station A to testing station B with a PN less than the current value minus the replayWindow value.
4. Observe the frames received by testing station B.
5. Transmit a frame from testing station A to testing station B with a PN 1024 greater than the nextPN for the SA.
6. Observe the frames received by testing station B.
7. Transmit a frame from testing station A to testing station B with a PN 1023 less than the frame used in step 5.
8. Observe the frames received by testing station B.

If the DUT is an end station:

9. Transmit an ICMP Echo Request from testing station A to the DUT with a PN that is the correct next number for that SA.
10. Observe the frames received by testing station A.

11. Transmit an ICMP Echo Request testing station A to the DUT with a PN less than the current value minus the replayWindow value.
12. Observe the frames received by testing station A.
13. Transmit an ICMP Echo Request from testing station A to the DUT with a PN 1024 greater than the nextPN for the SA.
14. Observe the frames received by testing station A.
15. Transmit an ICMP Echo Request from testing station A to the DUT with a PN 1023 less than the frame used in step 13.
16. Observe the frames received by testing station A.

Observable Results:

a. In steps 2 and 6, testing station B should receive the forwarded frames from testing station A.
b. In steps 3 and 8, testing station B should not receive the forwarded frames.
c. In steps 10 and 14, testing station A should receive an ICMP Echo Reply.
d. In steps 12 and 16, the DUT should not respond to the ICMP Echo Requests.

Possible Problems: If the DUT does not allow replayProtect to be enabled, this test cannot be performed.